Panda Antivirus Server

for Mac

User Manual

Legal information

Use of this product is subject to acceptance of the Panda Security End User License Agreement enclosed.

Panda Security™ is registered in the US Patent and Trademark office. the United States and other countries.

Panda Security, S.L., Gran Vía Don Diego López de Haro 4, 48001 Bilbao, Spain.

© Panda Security 2010. All rights reserved.

TABLE OF CONTENTS

LEGAL INFORMATION 2

WHAT IS PANDA ANTIVIRUS SERVER FOR MAC? 4

MANAGING PANDA ANTIVIRUS SERVER FOR MAC 5

Installing Panda Antivirus Server on Your Server 5

Serializing Panda Antivirus Server 6

Updating Panda Antivirus Server 8

USING PANDA ANTIVIRUS SERVER 10

Scanning Your Entire Server for Malware 11

To Scan a Portion of Your Server for Malware 13

When Malware is Found 16

Examining Quarantined Files 17

Looking at Past Scans and Actions Taken 20

Changing the Program's Behavior 23

Running Panda Antivirus Server From the Command Line 25

TECHNICAL SUPPORT 28

What is Panda Antivirus Server for Mac?

Panda Antivirus Server for Mac provides protection from malware to users of Mac OS X Server, detecting and eliminating all types of malware:

- **Mac viruses**
- **Windows and Unix viruses**, which Mac users may unwittingly pass on to friends or colleagues
- **Trojan horses**, which are programs that hide their damaging effects behind useful functions
- **Macro viruses** found in Microsoft Word and Excel documents
- **Worms**, which use your computer as a platform for damaging others across a network
- **Spyware and keyloggers**, which secretly watch what you do on your computer, potentially stealing valuable information such as passwords and credit-card numbers
- **Adware**, which displays non-removable advertisements on your computer
- **Hacking tools** that allow criminals to gain access to your computer
- **Dialers**, which force you to pay for unauthorized telephone access charges
- **Scareware**, which holds your computer hostage until you pay a clean-up fee

Panda Antivirus Server includes a subscription for automatic updates, so you're protected against new attacks as they appear. It silently checks every new and changed file for threats, so you never have to do anything to stay protected. You can get added peace of mind by ordering it to scan your entire hard disk, or any part of it, whenever you like.

Panda Antivirus Server runs on any officially supported Mac OS X Server compatible computer with at least 80 MB of free hard disk space, running Mac OS 10.5 or later or Mac OS X Server 10.5 or later. Panda Antivirus Server runs in 64-bit mode on Mac OS X 10.6 or Mac OS X Server 10.6 if the Mac where it is installed has at least 2 GB RAM (otherwise it runs in 32-bit mode).

Managing Panda Antivirus Server for Mac

Installing Panda Antivirus Server on Your Server

Double-click the Panda Antivirus Server.pkg file you downloaded or received on disc. The Mac OS X Installer program will launch. Follow the instructions presented by this program. When the installer has completed, you'll need to restart your Mac.

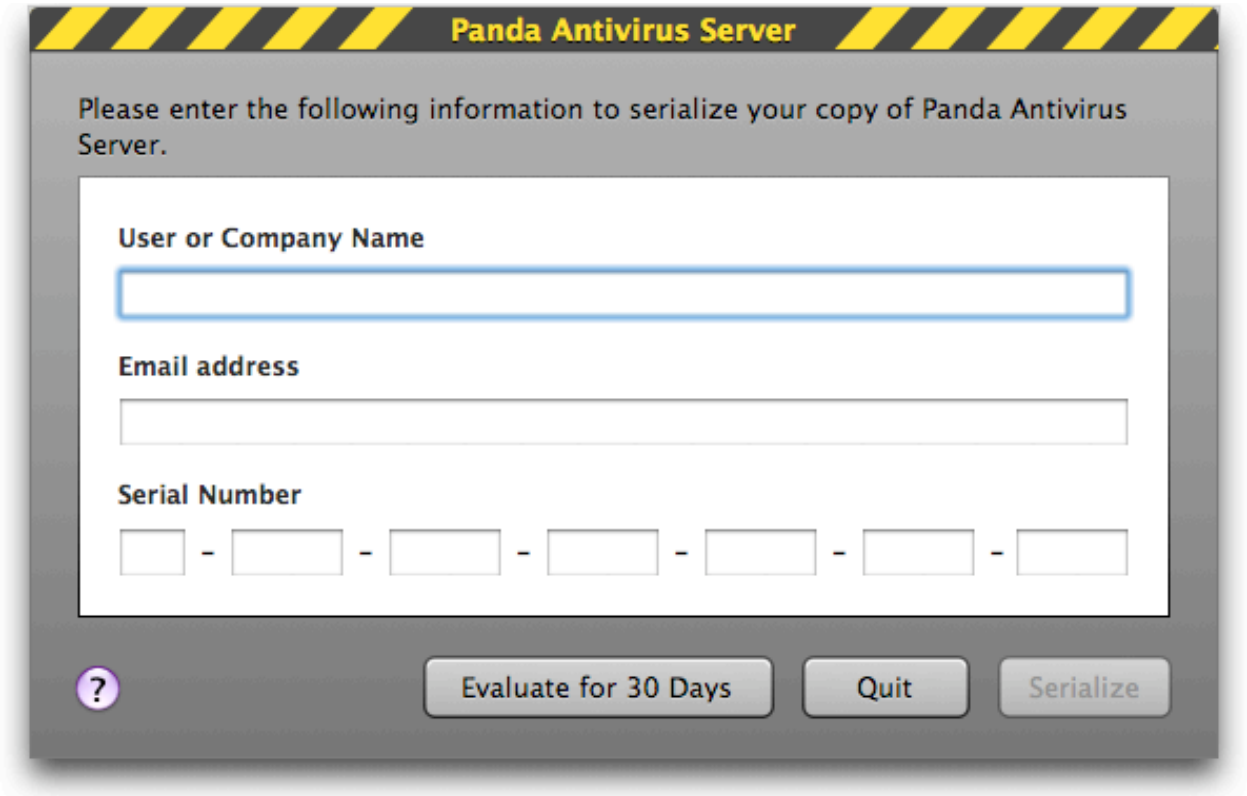
You can also install Panda Antivirus Server remotely using Apple Remote Desktop, or via the command line, using the `installer` tool.

If you ever need to uninstall Panda Antivirus Server, you can use the Uninstaller application on the disk image that contains the installer, or you can run the following script via the command line:

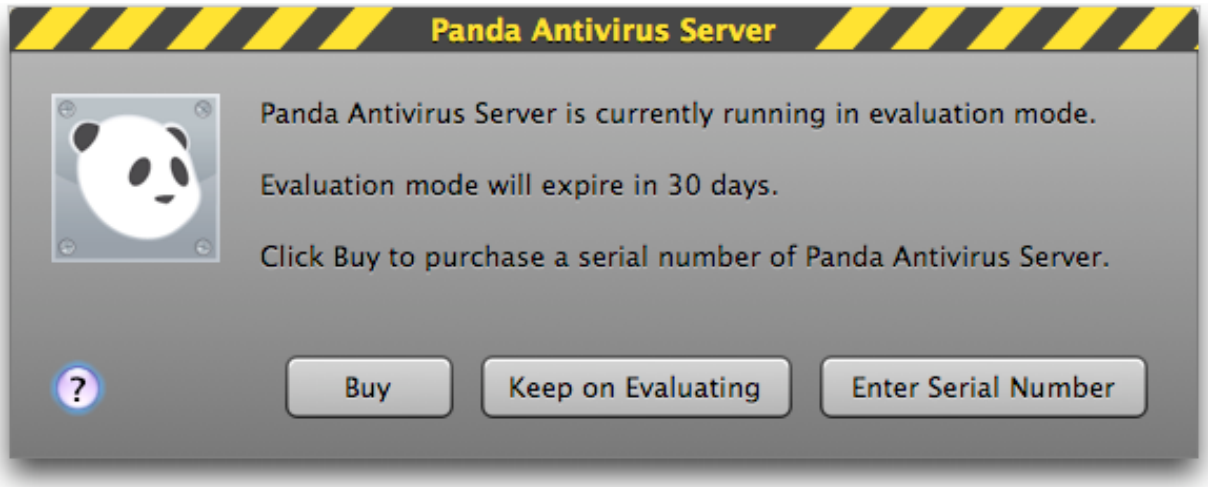
```
sudo sh /Library/Panda\ Security/Antivirus/uninstall.sh
```

Serializing Panda Antivirus Server

When you first launch Panda Antivirus Server, which is in the Applications folder, you'll see a window that asks for your name, email address, and serial number. (You received your serial number when you bought the product.) If you don't have a serial number—for example, if you'd like to try Panda Antivirus Server's free trial—click the **Evaluate for 30 Days** button. Otherwise, enter the information. When you're done, the **Serialize** button becomes available: click it to continue. (You can also click **Quit** at any time, although doing so means that Panda Antivirus Server won't be protecting your computer.)



If you've chosen the 30-day evaluation period, a warning window will appear every time you open the application during the trial period. From there you can **Enter Serial Number** (if you have one) to use the program permanently, **Buy** to purchase a serial number, or **Keep on Evaluating** to continue the your evaluation until your 30-day trial period runs out.

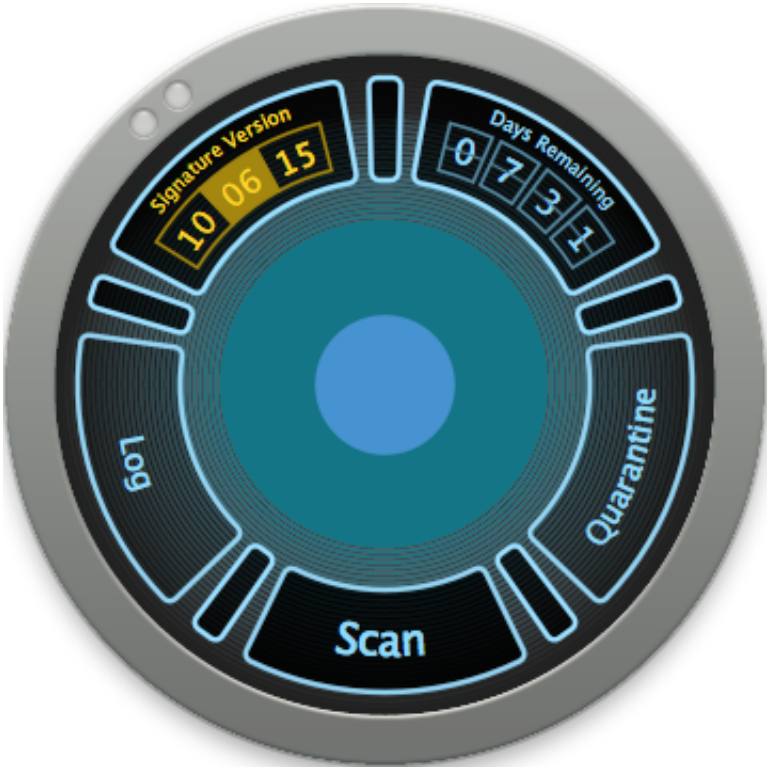

Panda Antivirus Server
Panda Antivirus Server is currently running in evaluation mode.
Evaluation mode will expire in 30 days.
Click Buy to purchase a serial number of Panda Antivirus Server.
Buy
Keep on Evaluating
Enter Serial Number

When the 30 days have expired, you'll see a window directing you to either **Buy** the product, **Enter Serial Number**, or **Quit**. (You can't continue using Panda Antivirus Server for Mac after the expiration of this trial period without a serial number.)

Updating Panda Antivirus Server

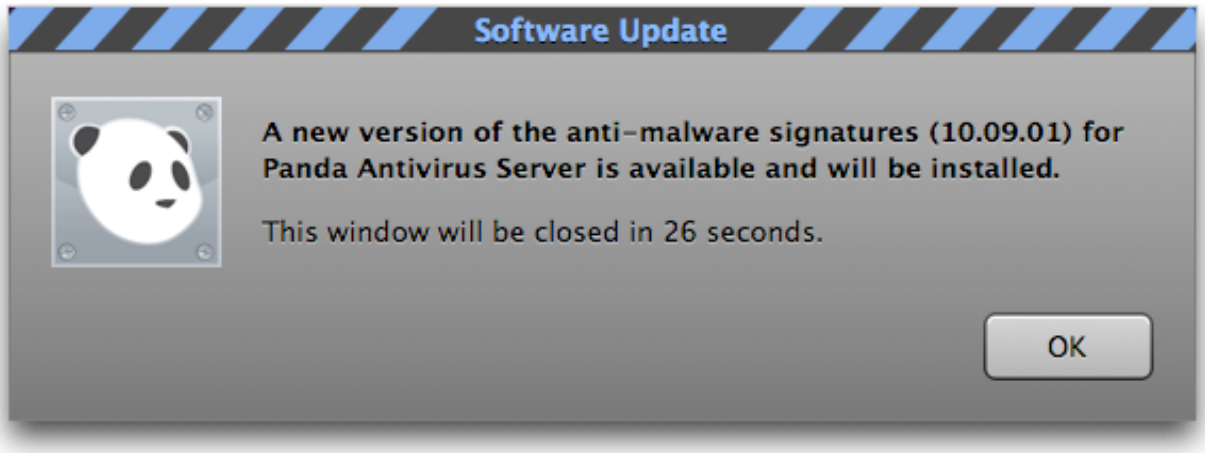
Malware creators work around the clock to find ways to attack your Mac. As soon as possible after a threat appears, we release an update for Panda Antivirus Server anti-malware signatures to spot and eliminate it.

If Panda Antivirus Server anti-malware signatures are up to date, the program displays the **Signature Version** number in blue. Panda Antivirus Server will display the **Signature Version** information in a different color if it notices that its signatures are outdated. This color will first be yellow, then orange, then red as the date of the last anti-malware signature update is further away from the present date.



Panda Antivirus Server will look for updates automatically once a day. You can also direct it to do so whenever you want by selecting **Check for Updates…** in the **Panda Antivirus Server** menu.

If there are updates to anti-malware signatures, you'll be informed of their availability and they will be installed automatically.


Software Update
A new version of the anti-malware signatures (10.09.01) for Panda Antivirus Server is available and will be installed.
This window will be closed in 26 seconds.
OK

If there are updates to the Panda Antivirus Server application, you will be informed of this, and will have the option to install the update or do it later. Updates to the Panda Antivirus Server require that you restart your Mac.

If there are no updates, you'll be informed of that fact.

Using Panda Antivirus Server

To keep your Mac OS X server protected against malware, all you need to do is install Panda Antivirus Server: it automatically checks every new and changed file on your computer, and all volumes connected to it, and quarantines dangerous files. However, you can also:

- Scan files at any time
- Look at past scans
- Examine files that Panda Antivirus Server has quarantined, and
- Change ways the program behaves

This section of the manual provides details for each of these functions, as well as describing what happens when Panda Antivirus Server finds a questionable file.

Scanning Your Entire Server for Malware

To scan your computer and all attached volumes for Malware, either click the Scan button on the Panda Antivirus Server scan disc, press Command–S, or select **Scan** from the **Scan** menu.

To stop a scan, click the **Stop** button, select **Stop** from the **Scan menu**, or press Command-S again. (The **Scan** command changes to **Stop** when a scan is running.)

You can move the Panda Antivirus Server window out of the way while it's scanning. To minimize the screen, click the small yellow button in the top-left area of the scan disc: Panda Antivirus Server will continue to perform the scan.

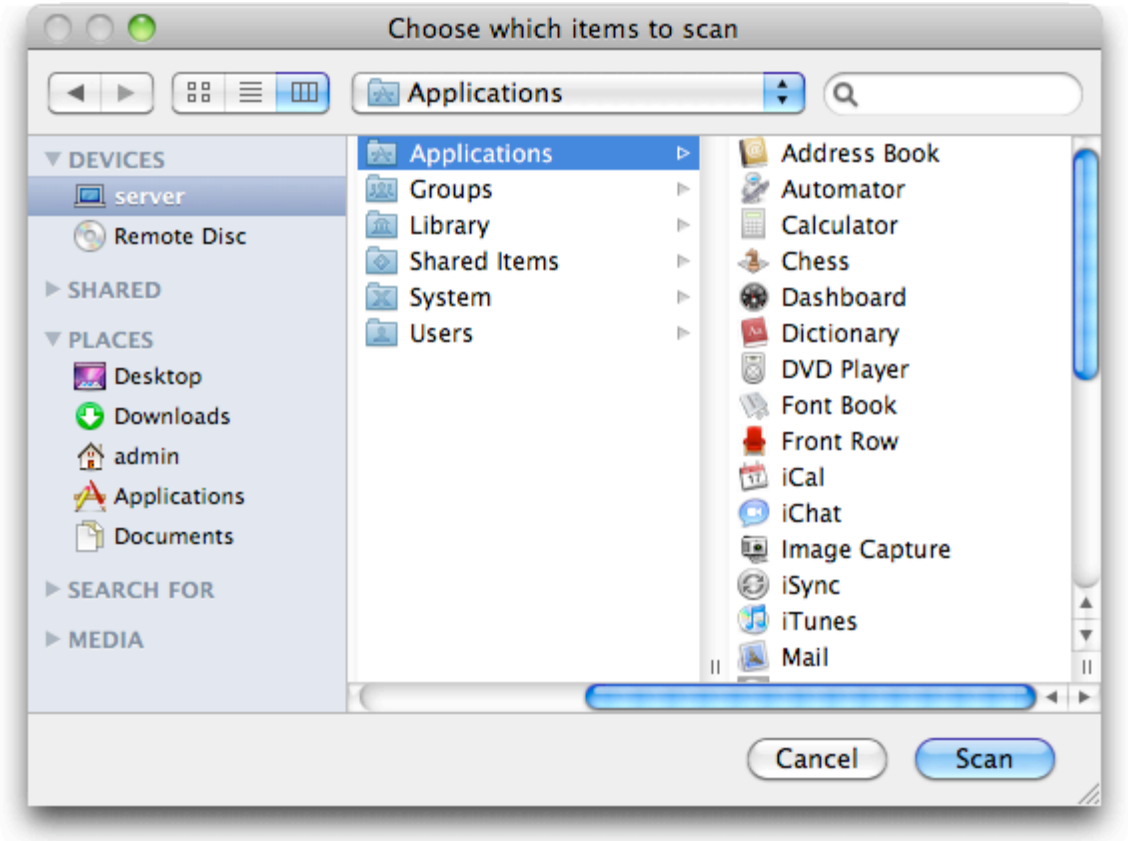
If you click on the Analyzing sector of the scan disc, it will expand showing you more information about files being scanned: you'll see the last part of the path leading to it, and the number of analyzed files will be hidden. (To return the display to its previous state, click that area again.)

Analyzing
theme_print.css.php
css
original
Stop

To Scan a Portion of Your Server for Malware

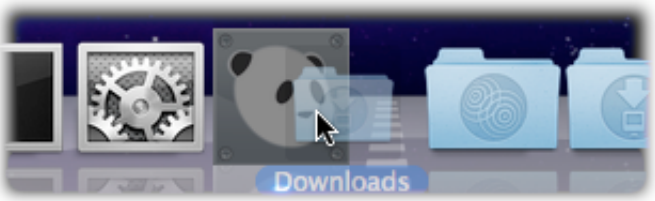
Panda Antivirus Server offers four methods to scan a portion of your server (or attached volumes) for malware. Either:

1. Select **Scan Custom Location…** from the **Scan** menu, or press Option-Command-S. A dialog box appears to let you choose the folder, volume, or file you'd like to check for malware. When ready, click **Scan**.

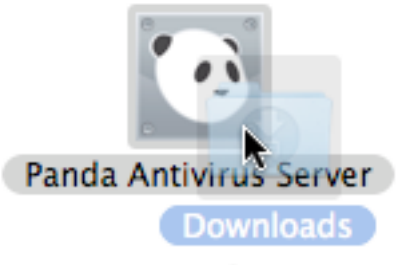


2. Drag the items onto the scan disc.

3. Drag the items onto Panda Antivirus Server's icon in the Dock.



4. Drag the items onto Panda Antivirus Server for Mac's icon in the Finder.



You can also scan an iPhone, iPod touch or iPad. To do so, connect the device to your computer, then choose **Scan iPhone/iPod touch** from the **Scan** menu. This displays a sub-menu showing the names of any such devices that are available. Choose the device, and Panda Antivirus Server for Mac will scan it, the same as it does for a folder or your entire Mac. (Note that scanning an iPhone, iPod touch or iPad may take a long time. Panda Antivirus Server has to copy all the files from the device to be able to scan them.)

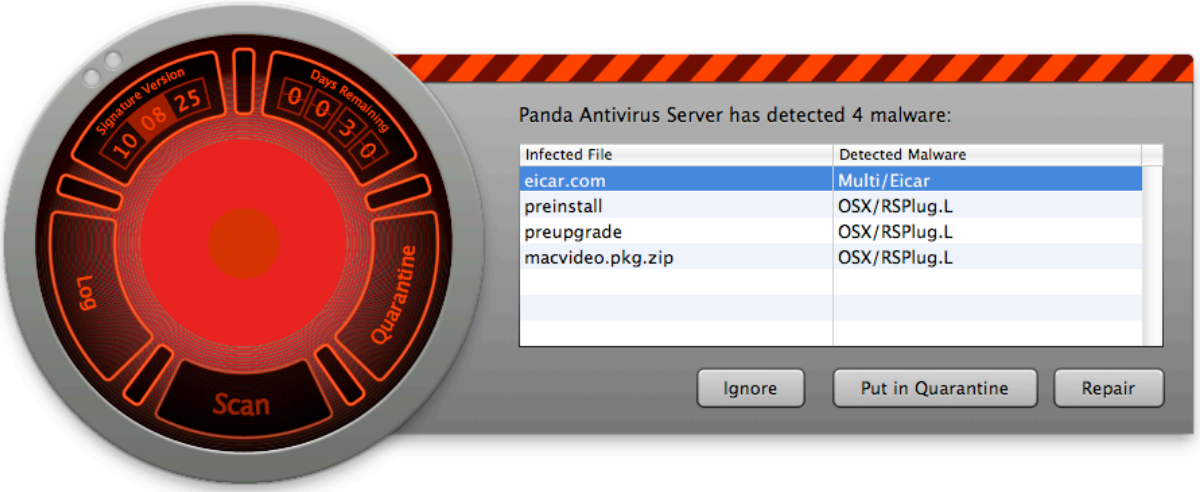
Regardless of whether you're scanning your server, a folder, or an iPhone/iPod touch, Panda Antivirus Server's main screen shows you the scan's progress. The area in the upper left tells you the name of the file currently being examined.

Some files are stored as archives in a compressed format, and must be uncompressed before being examined: for these files, the word "Analyzing" changes to "Unarchiving". (You can tell Panda Antivirus Server not to look inside such archives by unchecking **Scan archives** in the Preferences window. For more information, see the "Changing the Program's Behavior" section of this manual, below.)

A message appears if the scan reveals no problematic files.

When Malware is Found

If Panda Antivirus Server finds malware during a manual scan, the dialog looks like this:



You have three options:

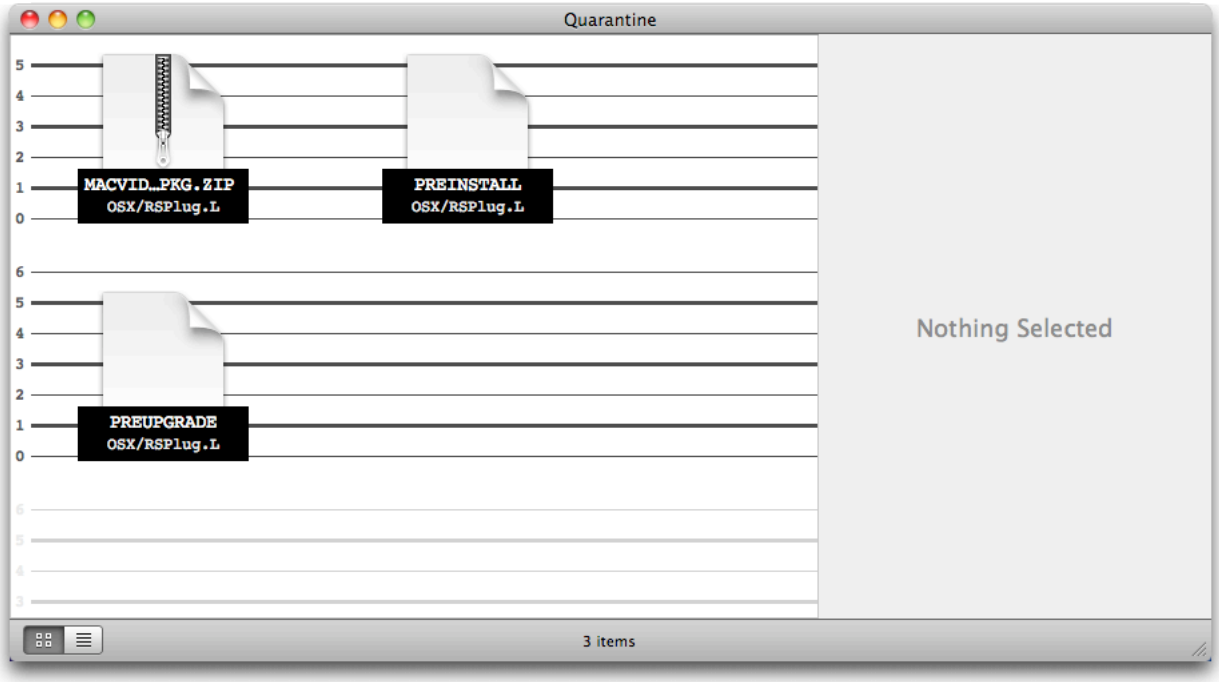
- **Ignore** the file, which leaves it on your server. Doing so might allow malware to damage your computer. Only click **Ignore** for files that you're certain aren't malware.
- **Put in Quarantine** segregates the file in an area where it cannot run or be opened, and therefore can't damage your computer. The Quarantine feature is only available if the program's on-access scanner is enabled.
- **Repair** removes the malware from the file, if this is possible. If not, the program deletes the file.

If Panda Antivirus Server finds malware when files are added or copied to your server via its on-access scanner, the files are either repaired or put in Quarantine, depending on which option you have chosen in the program's preferences. For more on this option, see **Changing the Program's Behavior** later in this manual.

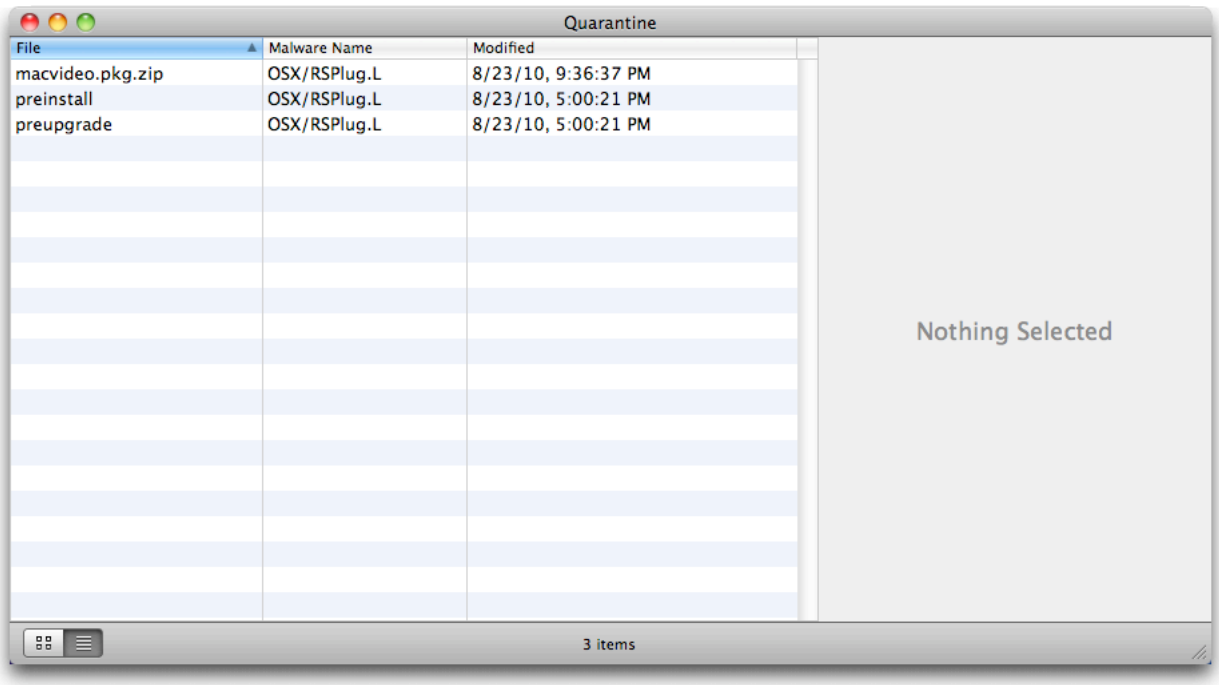
Examining Quarantined Files

You can examine files that have been placed in Quarantine by clicking the **Quarantine** button. (This button is only available when no scan is running.) You can also see the Quarantine by selecting **Quarantine** from the **Window** menu or by pressing Option-Command-2.

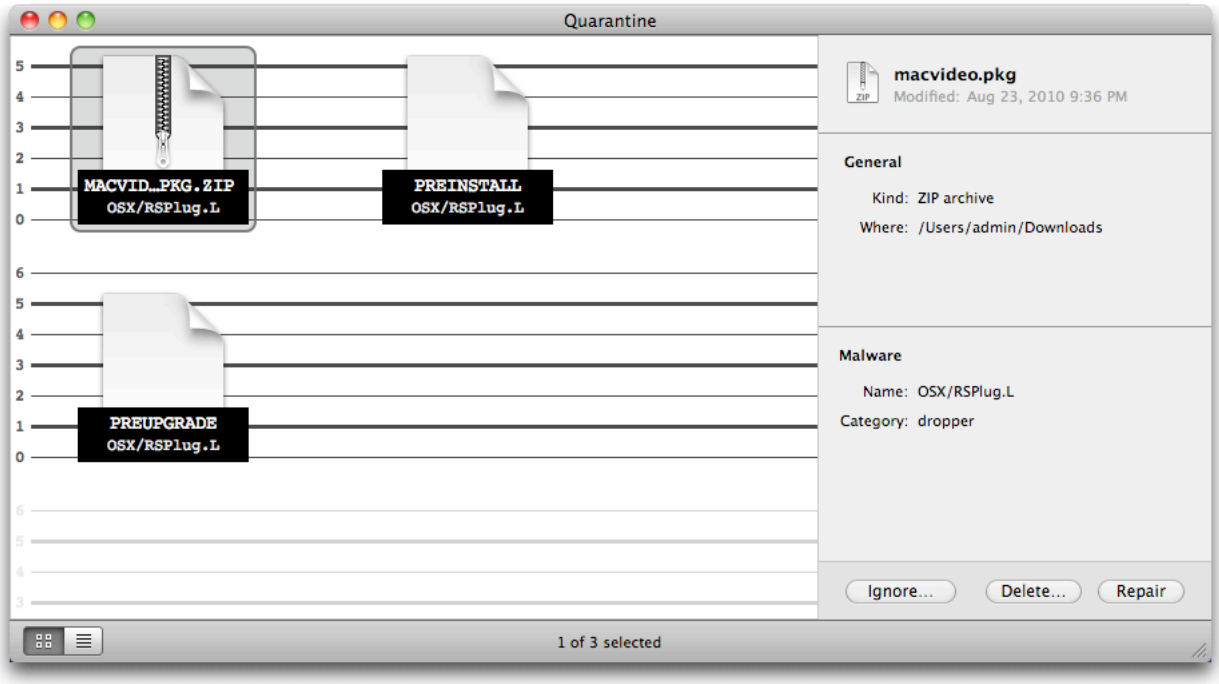
A window appears, showing all files that Panda Antivirus Server has quarantined.



This is the “mug shot” view that shows each file as an icon. To see them in a more compact, information-rich list format, click the second icon in the bottom-left corner. In List view, you can sort items according to their File names, Malware names, or Modified dates by clicking the header at the top of the appropriate column.



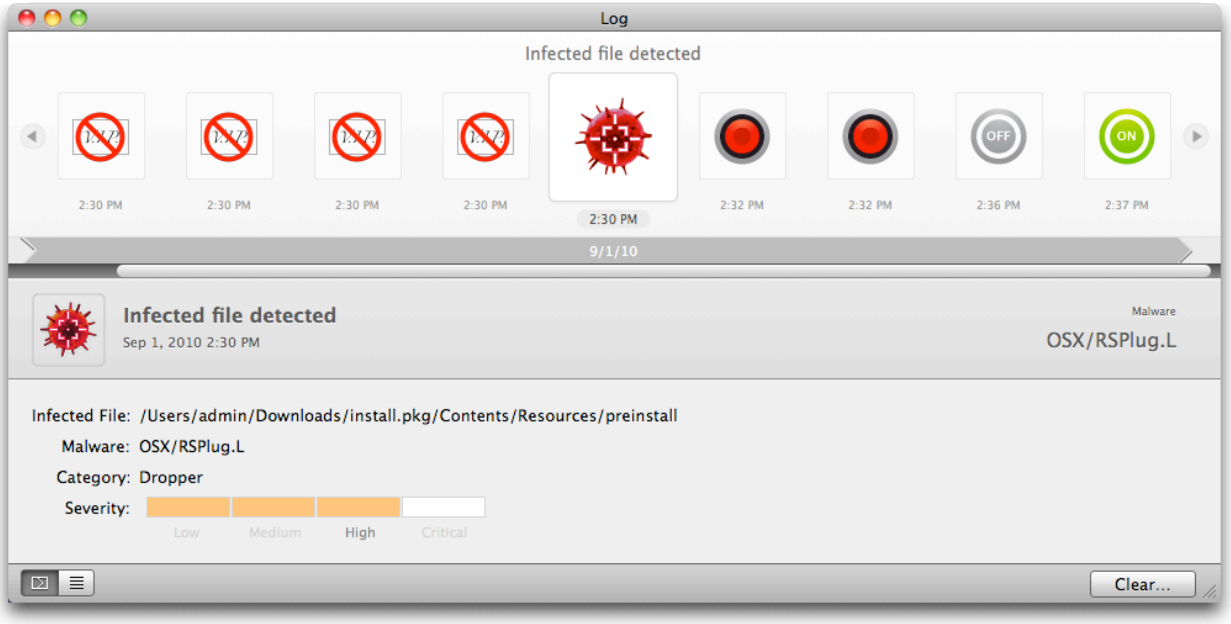
In either case, clicking an item in the main part of the window displays further information in the pane to the right. (If you select multiple items, the right pane tells you only how many items you selected.)



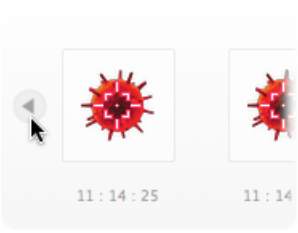
When items are selected, Panda Antivirus Server gives you the same three options as when it found the malware: **Ignore**, **Delete**, or **Repair**. After you choose to take any of these actions, the selected items disappear from the Quarantine, as they're no longer awaiting your decision.

Looking at Past Scans and Actions Taken

To see a record of scans already performed, and decisions you made regarding questionable files, either click the **Log** button, select **Log** from the **Window** menu, or press Command-Option-1. The Log window appears.



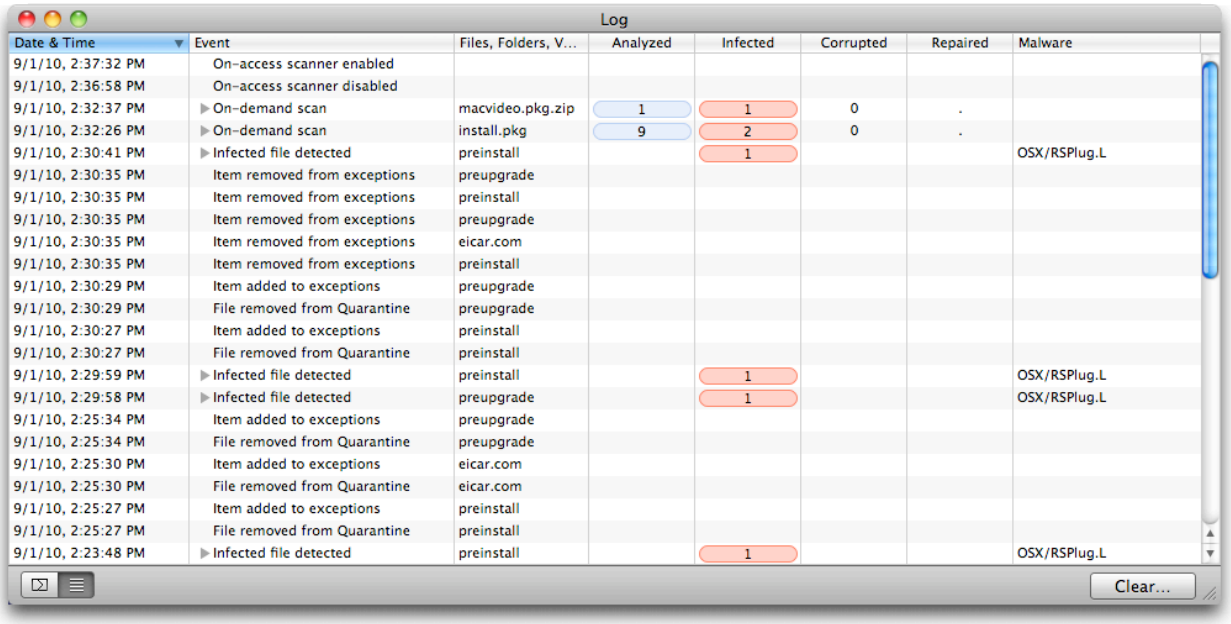
The top section of this window is a timeline of actions Panda Antivirus Server has taken, with earlier actions to the left. Each action is depicted with an icon, with the action's time below it. (The action's date is shown in a bar below the timeline.) Clicking an icon shows details of that action in the bottom pane. You can scroll through the timeline by clicking the small arrows on the right or left of it.



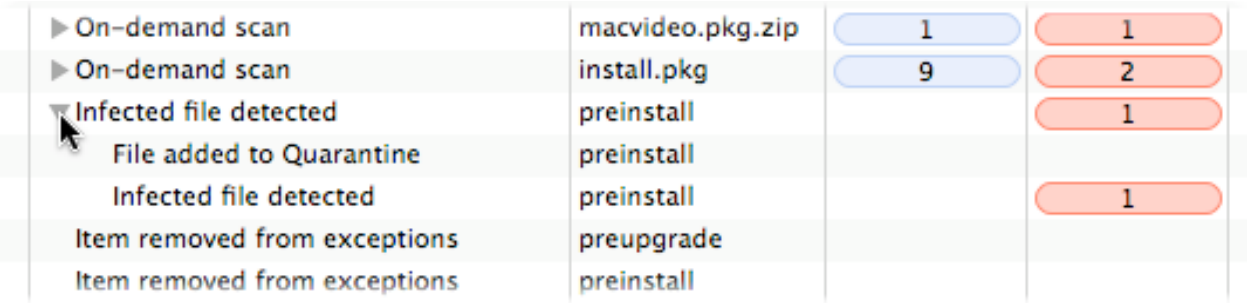
Another way of looking at the Log is as a list, which is more compact and shows more information. To see it, click the List view icon in the bottom-right of the Log window.

Details provided in the List view that aren't in the Timeline view include:

- Which files, folders, or volumes were affected by the action. (Hovering your cursor over this area shows you the item's full path.)
- The number of files that were analyzed; found to be infected by malware or corrupted; and repaired by Panda Antivirus Server
- The name of malware discovered, if any.


Log
Date & Time
Event
Files, Folders, V...
Analyzed
Infected
Corrupted
Repaired
Malware
9/1/10, 2:37:32 PM On-access scanner enabled
9/1/10, 2:36:58 PM On-access scanner disabled
9/1/10, 2:32:37 PM On-demand scan macvideo.pkg.zip 1 1 0 .
9/1/10, 2:32:26 PM On-demand scan install.pkg 9 2 0 .
9/1/10, 2:30:41 PM Infected file detected preinstall 1 OSX/RSPlug.L
9/1/10, 2:30:35 PM Item removed from exceptions preupgrade
9/1/10, 2:30:35 PM Item removed from exceptions preinstall
9/1/10, 2:30:35 PM Item removed from exceptions preupgrade
9/1/10, 2:30:35 PM Item removed from exceptions eicar.com
9/1/10, 2:30:35 PM Item removed from exceptions preinstall
9/1/10, 2:30:29 PM Item added to exceptions preupgrade
9/1/10, 2:30:29 PM File removed from Quarantine preupgrade
9/1/10, 2:30:27 PM Item added to exceptions preinstall
9/1/10, 2:30:27 PM File removed from Quarantine preinstall
9/1/10, 2:29:59 PM Infected file detected preinstall 1 OSX/RSPlug.L
9/1/10, 2:29:58 PM Infected file detected preupgrade 1 OSX/RSPlug.L
9/1/10, 2:25:34 PM Item added to exceptions preupgrade
9/1/10, 2:25:34 PM File removed from Quarantine preupgrade
9/1/10, 2:25:30 PM Item added to exceptions eicar.com
9/1/10, 2:25:30 PM File removed from Quarantine eicar.com
9/1/10, 2:25:27 PM Item added to exceptions preinstall
9/1/10, 2:25:27 PM File removed from Quarantine preinstall
9/1/10, 2:23:48 PM Infected file detected preinstall 1 OSX/RSPlug.L
Clear...

Some items have a disclosure triangle in the **Event** column; clicking it shows additional information.

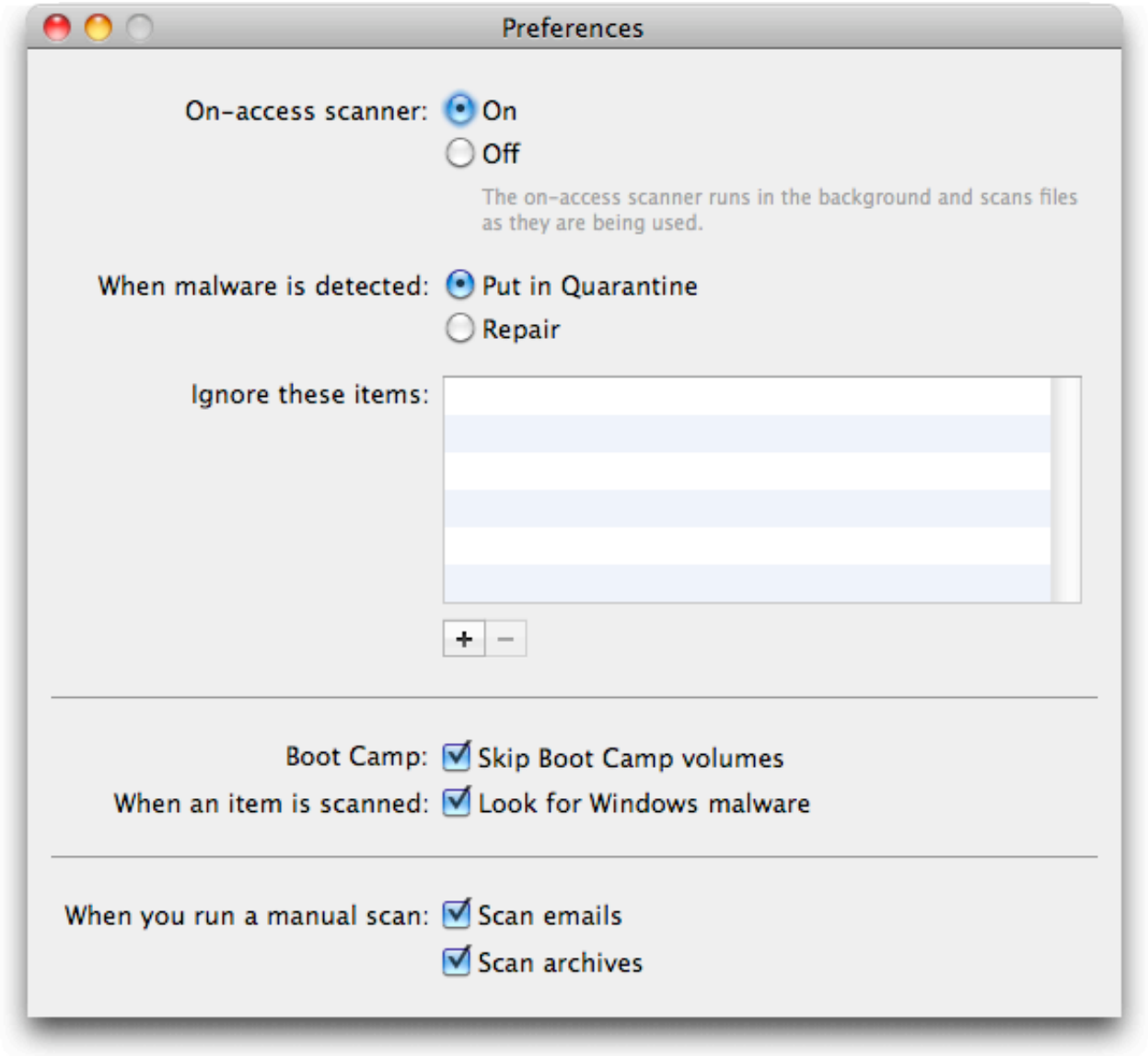


To remove all items from the Log, click the **Clear…** button in the bottom-right corner. This only removes the record of these actions from the Log window: it doesn't undo any previous actions, or initiate any new ones.

Changing the Program's Behavior

You can change some of Panda Antivirus Server's behavior through options in the Preferences window, which you can view by selecting **Preferences…** from the **Panda Antivirus** menu, or by pressing Command-comma.

The Preferences window appears.



Its options are:

- Enable or disable the **On-access scanner**. When turned **On**, Panda Antivirus Server protects your server by examining every new or changed file on your server and all volumes attached to it. If you have Panda Antivirus Server open, you'll see a throbbing blue circle in the center of the scan disc when the On-access scanner is on. When turned **Off**, Panda Antivirus Server only examines files when you run a manual scan (by clicking the **Scan** button, for example).
- The options for **When malware is detected** tell Panda Antivirus Server to either move all questionable files automatically into the Quarantine or Repair them if possible.
- The area labeled **Ignore these items** lists files, folders, and volumes that you don't want Panda Antivirus Server to examine. You can add items to this list either by clicking the **+** sign below the area, or by dragging items into it from the Finder. This list also shows any items that Panda Antivirus Server previously found questionable, but for which you clicked the **Ignore** button.
- The **Skip Boot Camp volumes** lets you tell Panda Antivirus Server to ignore any volumes set up using Apple's Boot Camp with Windows installations.
- The **When an item is scanned** area has a checkbox that lets you tell Panda Antivirus Server for Mac to **Look for Windows malware** — that is, files that could damage computers running Windows. Although these files can't damage your Mac OS X server directly, it's a good idea to leave this checkbox enabled to prevent such files from propagating on your network, and potentially infecting Windows PCs. However, unchecking this box may make your scans run faster.
- The **When you run a manual scan** area lets you choose whether to **Scan emails** and **Scan archives**. Unchecking either of these boxes will make scans run faster. Your computer will still be protected against threats in e-mails and archives on your computer archives as long as the **On** radio button is selected in the **On-access scanner** area.

Running Panda Antivirus Server From the Command Line

You can run Panda Antivirus Server for Mac from Mac OS X's command-line interface with the Mac OS X Terminal application, and integrate it into shell scripts if you desire. In many cases, you may find the command-line tool to be the best way to work with your server.

The command is located at:

`/Library/Panda Security/Antivirus/panda_av_scanner`

with the following usage:

usage: `panda_av_scanner [-rz] file ...`

`-r`: Scan then repair files

`-z`: Scan or repair archives

There is an additional command-line tool installed at `/usr/local/bin/panda_util`. This tool is used to get and change settings for the program. Its options are as follows:

usage: `panda_util object operation value ...`

```
object              operation          value(s)
-------------------------------------------------------
preferences                            show
-                   set                on-access on
-                   -                  -         off
-                   -                  behavior quarantine
-                   -                  -        repair
-                   -                  windows yes
-                   -                  -       no
-                   -                  skip-bootcamp yes
-                   -                  -             no
-                   -                  e-mails yes
-                   -                  -       no
-                   -                  archives yes
-                   -                  -        no
-                   add                exceptions file/folder
-                   remove             exceptions file/folder
-                   import             file
```

```
-                   export              file
quarantine          show
-                   ignore              file/folder
-                   repair              file/folder
-                   delete              file/folder
logs                show
-                   clear
update              check               signatures
-                   check               all
subscription        show
subscription        refresh
subscription        set                 name e-mail serial-number
version             show
```

Examples:

To deactivate scanning for Windows malware:

```
sudo panda_util preferences set windows no
```

To update anti-malware signatures, if an update is available:

```
sudo panda_util update check signatures
```

To display logs:

```
sudo panda_util logs show
```

To display the version of the program's anti-malware engine and signatures:

```
sudo panda_util version show
```

Information regarding specific commands:

`preferences show`: this displays the program's current settings; the terms in brackets are those that can be used to make changes using the command line.

`preferences add exceptions`: the final argument must be an absolute path to a file or directory.

`preferences remove exceptions`: same as above.

`preferences import`: this can be used to import preferences exported from another instance of the program to a .plist file. The final parameter must be an absolute path to the .plist file.

`quarantine ignore`: the final parameter, the file to be ignored, must be an absolute path.

`quarantine repair delete`: same as above.

`update check signatures`: checks for updates and updates anti-malware signatures even if there is a program update available.

`update check all`: checks for updates and updates both the program and anti-malware signatures, if available. If the server must be restarted following the update, this restart is performed. If a user is logged into the server, a dialog will display; if not, restart will occur automatically.

`subscriptions show`: displays the number of days remaining in the current subscription.

`subscription refresh`: can be used if the program's subscription has been updated but the program has not registered the update.

`subscription set`: can be used to serialize the program from the command line.

Technical support

Technical support is available from the **Help** menu. Choosing the first option, **Panda Antivirus Help**, displays this manual. The second, **Email Support**, creates a message in your preferred email program, addressed to our support department.

You can also request technical support by sending email to: PAV4MAC_English@pandasecurity.com

When sending a support request, include the version number of Panda Antivirus Server for Mac that you're using. You can find this by selecting **About Panda Antivirus** in the **Panda Antivirus** menu.

A window appears with the version number is in gray, under the words "Panda Antivirus".

Panda Antivirus Server
version 1.0 (53)
Powered by intego
Licensed to:
Remaining activation days:
365
Copyright © 2010 Intego. All rights reserved.
Panda Antivirus Server and the Panda icon are copyright of Panda Security.